Qualys PCI DSS

コンプライアンス プレイブック

2025 年 7 月 28 日

Qualys, Inc.

919 E Hillsdale Blvd

4th Floor

Foster City, CA 94404

1 (650) 801 6100

目　　次

改定履歴

Release Version	Release Date	Change Description
4.0.0	July 30, 2024	Initial Draft
4.0.0	February 04, 2025	The document is updated with the following changes • **Section – Requirement 12** - Added new requirement 12.3.3 in the compliance support diagram - Added new requirement 12.3.3 in the compliance support diagram
4.0.1	July 28, 2025	The document is updated with the following changes • **Section – Overview** - Updated the heading from Importance of PCI-DSS 4.0 to Importance of PCI-DSS Compliance • **Section – Requirement 6** - Added new requirement 6.4.3 in the compliance support diagram - Added new requirement 6.4.3 in the compliance support table • **Section – Requirement 11** - Added new requirement 11.6.1 in the compliance support diagram - Added new requirement 11.6.1 in the compliance support table

概要

ペイメントカード業界セキュリティ基準協議会（PCI-SSC）は、カード会員データを取り扱い、処理、転送するすべての組織および事業体が、PCI データセキュリティ基準 4.0（PCI-DSS 4.0）に準拠することを義務付けています。

PCI-DSS4.0 は、進化するセキュリティ脅威と技術に焦点を当てたシリーズの最新バージョンです。本基準は、カード会員データを保護するための運用上および技術上の要件も定義しています。

対象組織は、これらの要件を以下の 2 段階で実施する必要があります：

- 直ちに対応すべき要件：2024 年 3 月 31 日までに実施すること。
- 追加のベストプラクティス：2025 年 3 月 31 日までに実施すること。

PCI-DSS 準拠の重要性

PCI DSS 要件への準拠により、以下のことが保証されます：

1. 貴組織がカード会員データを保護するための最適なセキュリティ対策を実施していること
2. 貴社のブランドイメージ向上
3. セキュリティプログラムの基盤としての役割
4. 非準拠による連邦罰則の対象とならないことの保証

PCI 準拠の準備

以下は、組織が PCI 準拠を達成するための手順です。

1. PCI DSS 4.0 要件の分析
2. 組織のセキュリティ体制をレビュー
3. ギャップ分析
4. ソリューションの実装

PCI DSS 4.0 要件の分析

PCI DSS コンプライアンスを達成するために満たす必要がある主な要件を確認しましょう。

PCI DSS 4.0 ゴール	**PCI DSS 4.0 要件**
安全なネットワークとシステムを構築・維持	1. ネットワークセキュリティ管理を導入し、維持する
	2. すべてのシステムコンポーネントに安全な設定を適用する
アカウントデータを保護	3. 保存されたアカウントデータを保護する
	4. オープンなパブリックネットワークを介した送信中は、強力な暗号化技術を用いてカード会員データを保護する
脆弱性管理プログラムを維持	5. すべてのシステムとネットワークを悪意のあるソフトウェアから保護する
	6. 安全なシステムとソフトウェアを開発し、維持する
強力なアクセス制御対策を実施	7. 業務上の必要性に応じて、システムコンポーネントのカード会員データへのアクセスを制限する
	8. ユーザーを識別し、システムコンポーネントへのアクセスを認証する
	9. カード会員データへの物理的アクセスを制限する
ネットワークを定期的に監視・テスト	10. システムコンポーネントとカード会員データへのすべてのアクセスをログに記録し、監視する
	11. セキュリティシステムとネットワークを定期的にテストする
情報セキュリティポリシーを維持	12. ポリシーとプログラムによって情報セキュリティをサポートする

組織に適用される要件を特定します。PCI DSS 要件の詳細については、PCI DSS V4.0 Standard を参照してください。

組織のセキュリティ体制をレビュー

組織のセキュリティ体制を確認する手順は次のとおりです：

1. **セキュリティ要件の定義**：ビジネスニーズに応じて、組織のセキュリティ要件を明確に定義します。
2. **セキュリティ管理のテスト**：セキュリティポリシーと管理をテストし、セキュリティ要件を満たしていることを確認します。
3. **セキュリティリスクの特定**：すべての資産に対してセキュリティスキャンを実行し、セキュリティリスクを特定します。
4. **セキュリティ体制レポートの作成**：計画されたアクションと将来の参照のために、セキュリティ体制に関するすべての調査結果を文書化する必要があります。

ギャップ分析

組織のセキュリティ体制を確認したら、セキュリティ体制レポートの結果を PCI-DSS 4.0 の要件と比較します。この分析は、PCI-DSS 要件を満たすために必要なギャップと改善点を特定するのに役立ちます。

ソリューションの実装

ギャップ分析に基づいて、PCI DSS 要件を満たすベンダーを探すか、社内でソリューションを開発してください。
次のセクションでは、Qualys アプリケーションを使用してさまざまな PCI DSS 要件を満たす方法について説明します。

PCI コンプライアンスのための Qualys ソリューション

統合された Qualys アプリケーションスイートには、お客様の資産をあらゆるリスクから監視・保護するために設計された 20 以上のアプリケーションが含まれています。このセクションでは、PCI DSS コンプライアンスにおける様々な Qualys アプリケーションの役割と、組織に Qualys ソリューションを導入する手順について説明します。

Qualys セキュリティソリューションのセットアップ

組織向けに Qualys セキュリティ ソリューションを設定する手順は次のとおりです。

ステップ – 1: Qualys ユーザーアカウントの作成

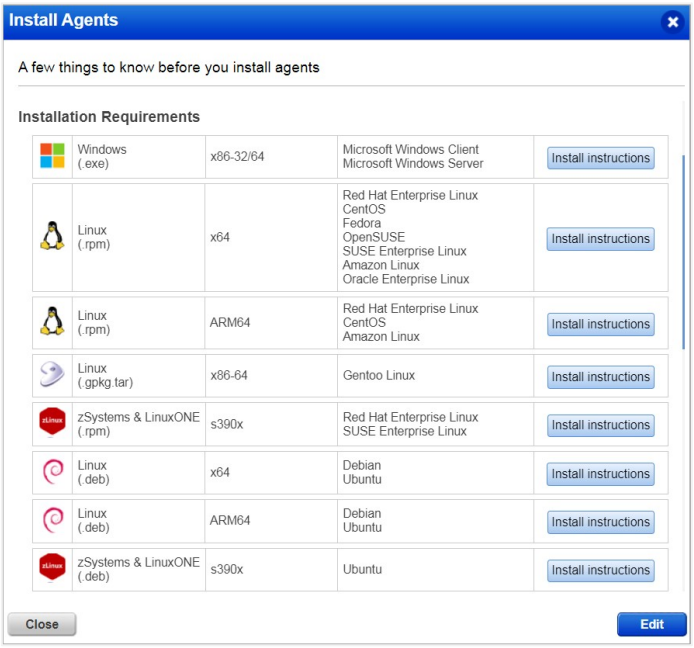
1. https://www.qualys.com でサインアップし、新しいユーザーアカウントを作成してください。既にアカウントをお持ちの場合は、Qualys の認証情報を使用して Qualys クラウドプラットフォームにログインしてください。
2. Qualys アプリケーションの使用を開始するには、必要なライセンスをすべてお持ちである必要があります。必要なライセンスをお持ちでない場合は、Qualys の担当者にお問い合わせください。

ステップ – 2: Cloud Agent とスキャナーをインストール

Cloud Agent とスキャナーは、資産のインベントリ構築を支援します。また、Qualys クラウドプラットフォームとの接続を確立し、資産データをアップロードします。

Qualys Cloud Agent のインストール

1. Qualys ユーザーアカウントで、Cloud Agent アプリケーションを開きます。
2. Cloud Agent UI から、ホストのシステムアーキテクチャに基づいて Cloud Agent インストーラパッケージをダウンロードします。

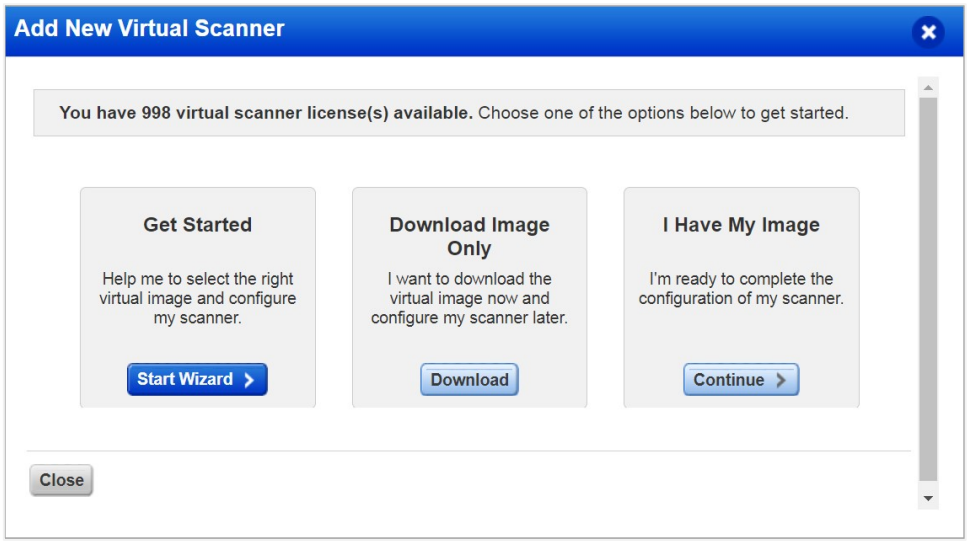


3. 必要なアセットに Cloud Agent をインストールしてください。Cloud Agent UI には、Cloud Agent のインストール手順の詳細が記載されています。
4. Cloud Agent の詳細については、Qualys Cloud Agent オンラインヘルプを参照してください。

スキャナーアプライアンスのデプロイメント

資産インベントリの全体像を把握するには、スキャナアプライアンスを導入する必要があります。スキャナアプライアンスを導入する手順は次のとおりです。

1. スキャナアプライアンスの UI から、スキャナアプライアンスをネットワークにインストールします。
2. ネットワーク設定を行い、スキャナが Qualys クラウドプラットフォームに接続されていることを確認します。



3. スキャナーアプライアンスの詳細については、スキャナーアプライアンスユーザーガイドおよび仮想スキャナ アプライアンスユーザーガイドを参照してください。

ステップ – 3: コンフィグレーション

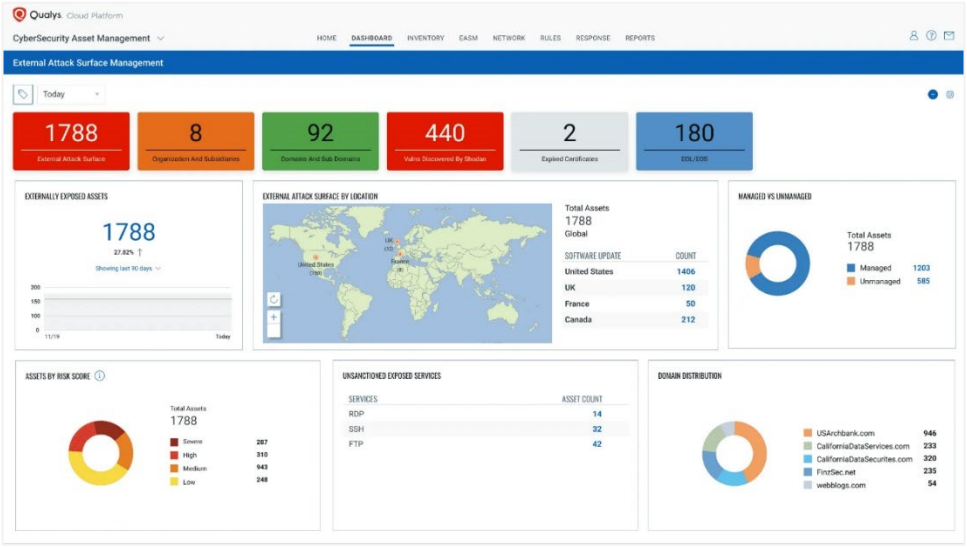
次のステップでは、アカウントの設定と資産インベントリの構築、コンフィグレーションプロファイルの作成、およびこれらのプロファイルを資産に適用します。このステップにおける重要なサブステップを以下に示します。

アセット管理

CSAM ダッシュボードでは、アセットインベントリの概要を確認できます。管理するには、Global AssetView アプリケーションに移動し、要件に基づいてアセットの分類を開始してください。

アセット管理を開始するには、以下の手順を実行します。

1. 機能、場所、重要度などの基準に基づいてアセットを分類し、タグ付けします。
2. スキャンおよびレポート作成用のアセットグループを設定する。

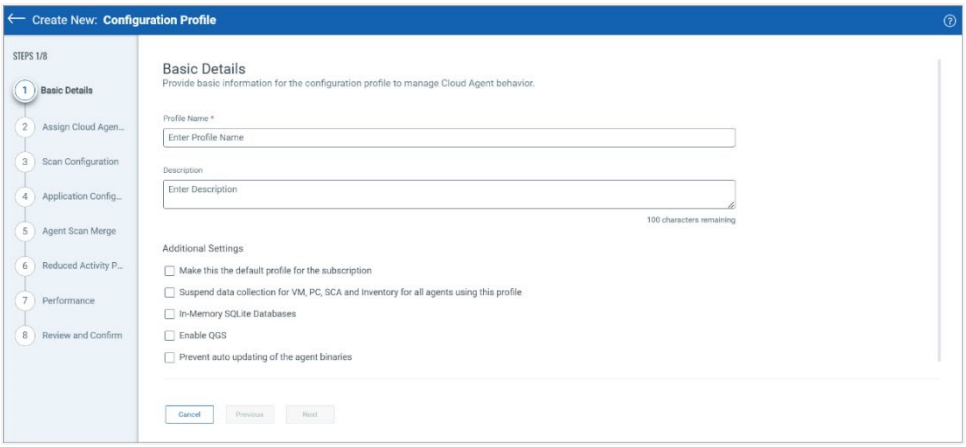


3. アセット管理の詳細については、CSAM オンラインヘルプおよび Global AssetView オンラインヘルプを参照してください。

コンフィグレーションプロファイルの作成

コンフィグレーションプロファイルを作成するオプションは、Cloud Agent UI で利用可能です。

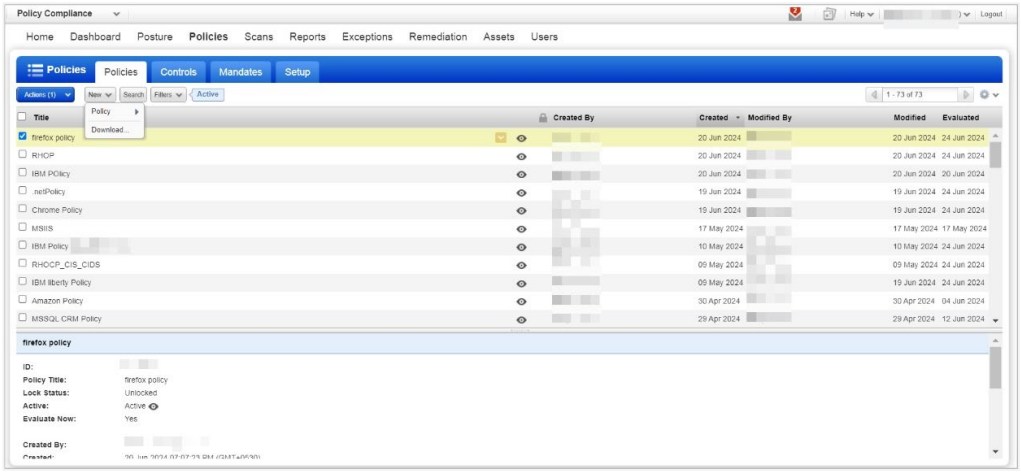
1. 異なるスキャン構成でコンフィグレーションプロファイルを作成します。



2. これらの構成プロファイルを、タグとグループを使用してアセットに適用します。
3. 構成プロファイルの作成について詳しくは、コンフィグレーションプロファイルの作成を参照してください。

ポリシーコンプライアンススキャンプロファイルの作成

1. ポリシーコンプライアンスアプリケーションで、要件に基づいてルールを定義します。
2. これらのポリシーコンプライアンスプロファイルを、タグを使用してアセットに適用します。



3. PC の詳細については、ポリシーコンプライアンス オンラインヘルプを参照してください。

アセットとネットワークの保護

Qualysセキュリティソリューションの設定が完了したら、次のステップはネットワークと資産が継続的に保護されていることを確認することです。以下のアプリケーションは、ネットワークと資産の保護を支援します。

VMDR Qualys Vulnerability Management, Detection, and Response (VMDR)

以下の VMDR 機能を使用して、資産とネットワークを保護できます:

- Qualys VMDR はすべての脆弱性を包括的に可視化し、優先順位付けルールと対応策を設定できます。
- VMDR はネットワーク上の全資産を OS、ポート、サービス、証明書などの詳細情報と共にマッピングし、脆弱性をスキャンします。
- VMDR は修正チケットの割り当て、例外管理、各ホストのパッチ一覧表示を行い、既存の IT チケットシステムと連携して検出された脆弱性を効果的に修正します。
- VMDR はネットワーク状態を記録する包括的なレポートを生成します。これらのレポートは VM API を使用して他のセキュリティおよびコンプライアンスシステムと連携できます。

Qualys VMDR の詳細については、Qualys VMDR オンラインヘルプを参照してください。

CM Continuous Monitoring (CM)

以下の VM 以下の Qualys CM 機能を使用して、資産とネットワークを継続的に監視できます:

- Qualys Continuous Monitoring (CM) はクラウドからグローバルネットワークを監視し、潜在的なリスクを適切な関係者に通知するターゲット型アラートを生成します。
- CM は、オンプレミスシステム、モバイルデバイス、パブリッククラウドインスタンスを監視できます。
- アラートのルールを異なる条件、対象、受信者に合わせて設定することも可能です。

Qualys CM の詳細については、Qualys Continuous Monitoring オンラインヘルプを参照してください。

PC SCA Policy Compliance (PC)

以下の Qualys PC 機能を使用して、ポリシーコンプライアンスルールを定義できます:

- Qualys Policy Compliance (PC) は、完全なポリシーコンプライアンスを実現する単一プラットフォームです。
- セキュリティ侵害や設定ミスのリスクを低減します。
- Qualys PC は、すべてのネットワークコンポーネントが安全に設定され、業界で認められた基準に準拠していることを保証します。

Qualys Qualys PC の詳細については、Qualys Policy Compliance オンラインヘルプを参照してください。

GAV File Integrity Monitoring (FIM)

以下の Qualys FIM 機能を使用して、資産とネットワークを保護できます:

- Qualys File Integrity Monitoring (CM) はグローバル IT システム全体における整合性違反とコンプライアンスを監視します。
- アラートのノイズを排除し、最も重大なインシデント、変更、悪意のあるイベントを優先的に対応するのに役立ちます。
- FIM にはファイルアクセス監視（FAM）が含まれ、重要なホストファイルへのアクセス時にアラートをトリガーします。エージェントレスネットワークサポートにより、ネットワーク構成の逸脱が検出された際にもアラートを生成します。
- FIM には PCI-DSS 4.0 やその他のコンプライアンス基準に準拠するための事前設定済み監視プロファイルも備わっています。

Qualys FIM の詳細については、Qualys File Integrity Monitoring オンラインヘルプを参照してください。

WAS Web Application Scanning (WAS)

以下の Qualys WAS 機能を使用して、Web アプリケーションを保護できます:

- Qualys Web Application Scanning (WAS) ツールは、最新の Web アプリケーションおよび API のリスクを最小限に抑え、攻撃対象領域を削減するのに役立ちます。
- 実行時脆弱性、OWASP トップ 10、設定ミス、個人識別情報(PII)の漏洩、Web マルウェアを検出するとともに、迅速な修正手順を提供します。

Qualys WAS の詳細については、Qualys Web Application Scanning オンラインヘルプを参照してください。

EDR Endpoint Detection and Response (EDR)

ネットワーク内のエンドポイントを保護するには、以下の Qualys EDR 機能を利用できます:

- EDR はエンドポイント上で不審な活動や潜在的な脅威を監視します。
- 悪意のあるソフトウェアからエンドポイントを保護するため、リアルタイムの検知と対応を提供します。

Qualys EDR の詳細については、Qualys Endpoint Detection and Response オンラインヘルプを参照してください。

PC SCA Security Congiguration Assessment (SCA)

以下の Qualys SCA 機能を使用して、資産とネットワークを保護できます:

- Qualys Security Configuration Assessment (SCA) では、Center for Internet Security (CIS) ベンチマークに基づいて、セキュリティ関連の問題を評価、報告、監視、修正できます。
- SCA を使用すると、IT 資産が CIS ガイドラインに従って安全に構成されているかどうかを継続的に確認できます。
- SCA はセキュリティ設定ツールとして機能するだけでなく、PCI-DSS、HIPAA などの基準への準拠を支援します。

Qualys SCA の詳細については、Qualys Security Configuration Assessment オンラインヘルプを参照してください。

PM Patch Management (PM)

アセットを最新の状態に保つには、以下の Qualys PM 機能を利用できます:

- PM を使用してパッチを展開し、システムとネットワークの更新を確実に実行できます。
- パッチジョブを作成し、パッチを選択して展開対象資産を指定することも可能です。

Qualys PM の詳細については、Qualys Patch Management オンラインヘルプを参照してください。

UD Unified Dashboard (UD)

以下の Qualys UD 機能を使用して、セキュリティコンプライアンス状況を確認できます:

- UD は組織のセキュリティおよびコンプライアンス状況を統合的に表示します。
- 各種 Qualys モジュールのデータをカスタマイズ可能なダッシュボードに統合し、リアルタイムの洞察と可視化を提供します。
- 単一のインターフェースから主要指標の追跡、脆弱性の監視、コンプライアンス状況の評価が可能です。

Qualys UD の詳細については、Qualys Unified Dashboard オンラインヘルプを参照してください。

SAQ Security Assessment Questionnaire (SAQ)

Qualys SAQ は以下の機能を提供します:

- SAQ はセキュリティ評価とコンプライアンス調査の実施プロセスを効率化し自動化します。
- 社内チーム、パートナー、ベンダーからセキュリティ慣行、コンプライアンス状況、リスク管理に関する情報を収集するため、質問票を作成、配布、分析します。
- SAQ は包括的なデータ収集と分析を通じて、徹底的かつ一貫した評価の確保、規制コンプライアンスの支援、セキュリティリスクの特定と軽減を支援します。

Qualys SAQ の詳細については、Qualys Security Assessment Questionnaire オンラインヘルプを参照してください。

CAR Custom Assessment and Remediation (CAR)

Qualys CAR は、セキュリティおよびコンプライアンス評価を管理するための以下の機能を提供します:

- CAR では、カスタムセキュリティおよびコンプライアンス評価と修復ワークフローの作成および自動化が可能です。
- 特定のセキュリティチェックの定義、詳細なレポートの生成、独自の環境と要件に合わせた修復タスクの自動化を支援します。
- CAR は、様々なアセットにわたるセキュリティ設定と脆弱性に対するリアルタイムの可視性と制御を提供することで、セキュリティ体制の改善を支援します。

Qualys CAR の詳細については、Qualys Custom Assessment and Remediation オンラインヘルプを参照してください。

CERT Certificate View

Qualys Certificate View は、証明書管理のために以下の機能を提供します:

- Certificate View は、組織の IT 環境全体にわたるデジタル証明書の包括的な可視性と管理を実現します。
- SSL/TLS 証明書の特定、追跡、監視を支援し、適切に構成され有効期限が切れていないことを保証します。
- Certificate View は、自動スキャン、詳細なレポート、アラートを提供し、安全でコンプライアンスに準拠した証明書インフラの維持を支援します。

Qualys Certificate View の詳細については、Qualys Certificate View オンラインヘルプを参照してください。

ADMIN Administration

Qualys Administration は、システム管理のために以下の機能を提供します:

- Qualys Administration は、Qualys Cloud Platform 全体におけるユーザーアクセス、ロール、権限の管理を支援します。
- 管理者は、セキュリティ設定の構成と制御、ユーザーロールの割り当て、資産の管理、プラットフォーム使用状況の監視を行うことができます。
- Qualys Admin は、安全かつ効率的なプラットフォーム管理の確保を支援し、組織内でのセキュリティポリシーとコンプライアンス要件の施行を促進します。

Qualys Administration の詳細については、Qualys Administration オンラインヘルプを参照してください。

TC Qualys TotalCloud

Qualys TotalCloud は、お客様の資産とネットワークを保護するために以下の機能を提供します:

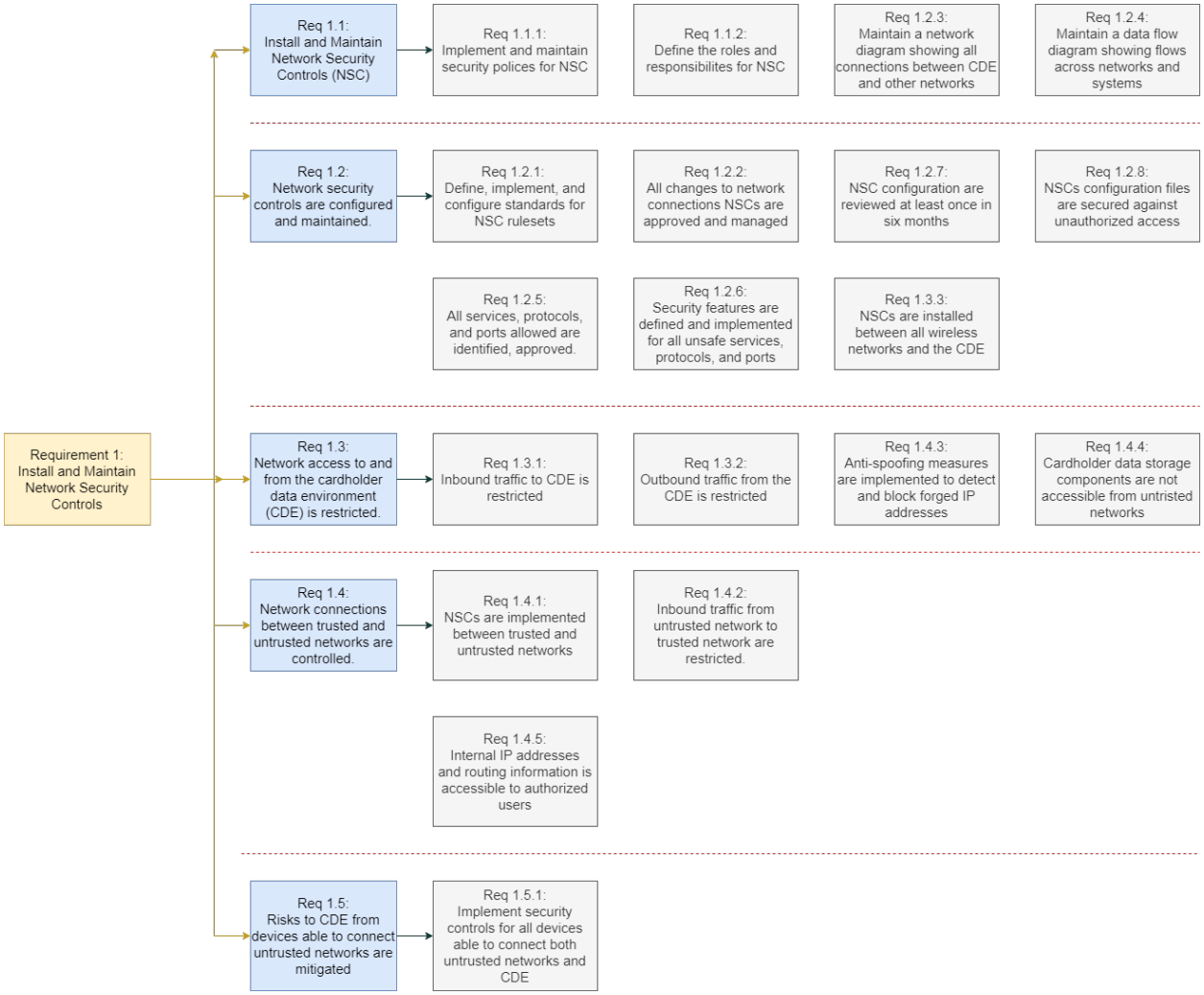
- Qualys TotalCloud は、クラウド環境に対する可視性、コンプライアンス、保護を提供する包括的なクラウドセキュリティソリューションです。
- 様々なクラウドプラットフォームと連携し、リアルタイム監視、脆弱性管理、コンプライアンスチェックを提供します。
- TotalCloud は、設定ミスを検知し、脆弱性を特定し、業界標準への準拠を確保することで、クラウドインフラのセキュリティ強化を支援します。
- 自動化されたワークフローと集中管理によりクラウドセキュリティ管理を簡素化し、クラウド資産の全体的なセキュリティ体制を強化します

Qualys TotalCloud の詳細については、Qualys TotalCloud オンラインヘルプを参照してください。

PCI コンプライアンスサポート

PCI DSS 要件 1

ネットワーク セキュリティ制御をインストールして維持: カード所有者のデータを不正アクセスから保護し、信頼できるネットワークと信頼できないネットワーク間の接続を制御し、信頼できないネットワークとカード所有者データ環境 (CDE) の両方に接続できるデバイスによってもたらされるリスクを軽減する、安全なネットワーク インフラストラクチャを確立して維持することが重要です。



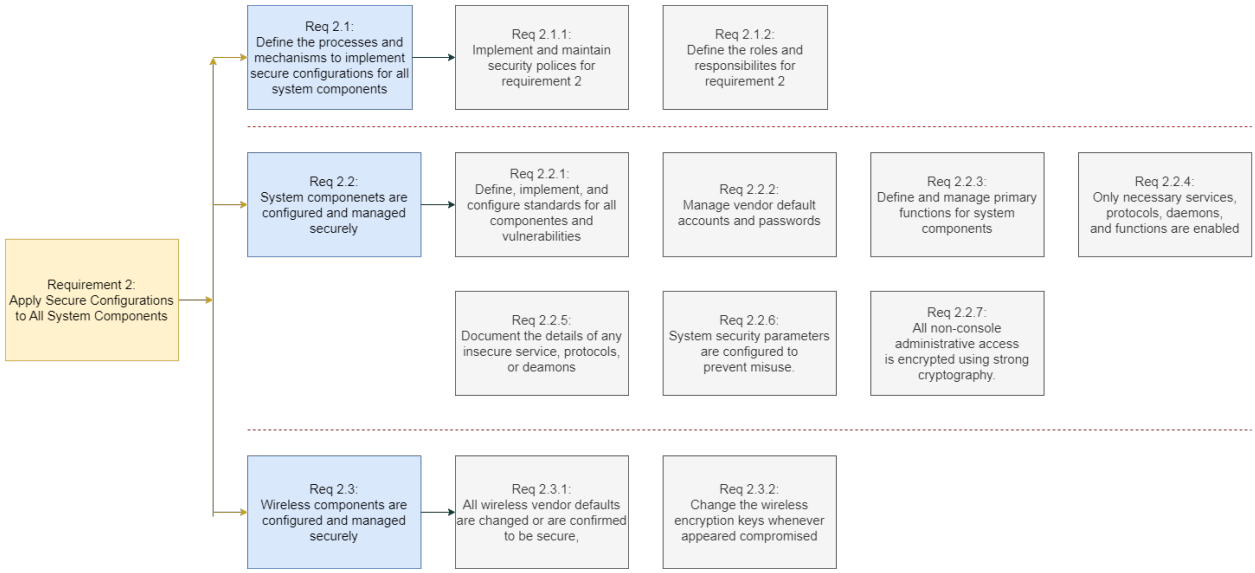
要件 1 のための Qualys ソリューション VMDR, CM, PC, FIM, EDR, SCA, PM, UD, GAV, CSAM

要件 1 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
1.2.1	✓								✓			
1.2.2			✓		✓							
1.2.6	✓		✓		✓	✓			✓			
1.2.8		✓	✓								✓	
1.3.1		✓	✓		✓				✓			
1.3.2		✓			✓						✓	
1.3.3		✓			✓				✓			
1.4.1		✓	✓		✓				✓			
1.4.2		✓			✓							
1.4.3	✓	✓			✓				✓			
1.4.4		✓	✓		✓				✓			
1.4.5		✓	✓								✓	
1.5.1	✓	✓	✓		✓	✓	✓	✓	✓		✓	

PCI DSS 要件 2

すべてのシステム コンポーネントに安全な構成を適用: 悪意のある人物がデフォルトのシステム構成の永続的な脆弱性を悪用するのを防ぐために、すべてのシステム コンポーネントとワイヤレス環境に安全な構成を実装します。



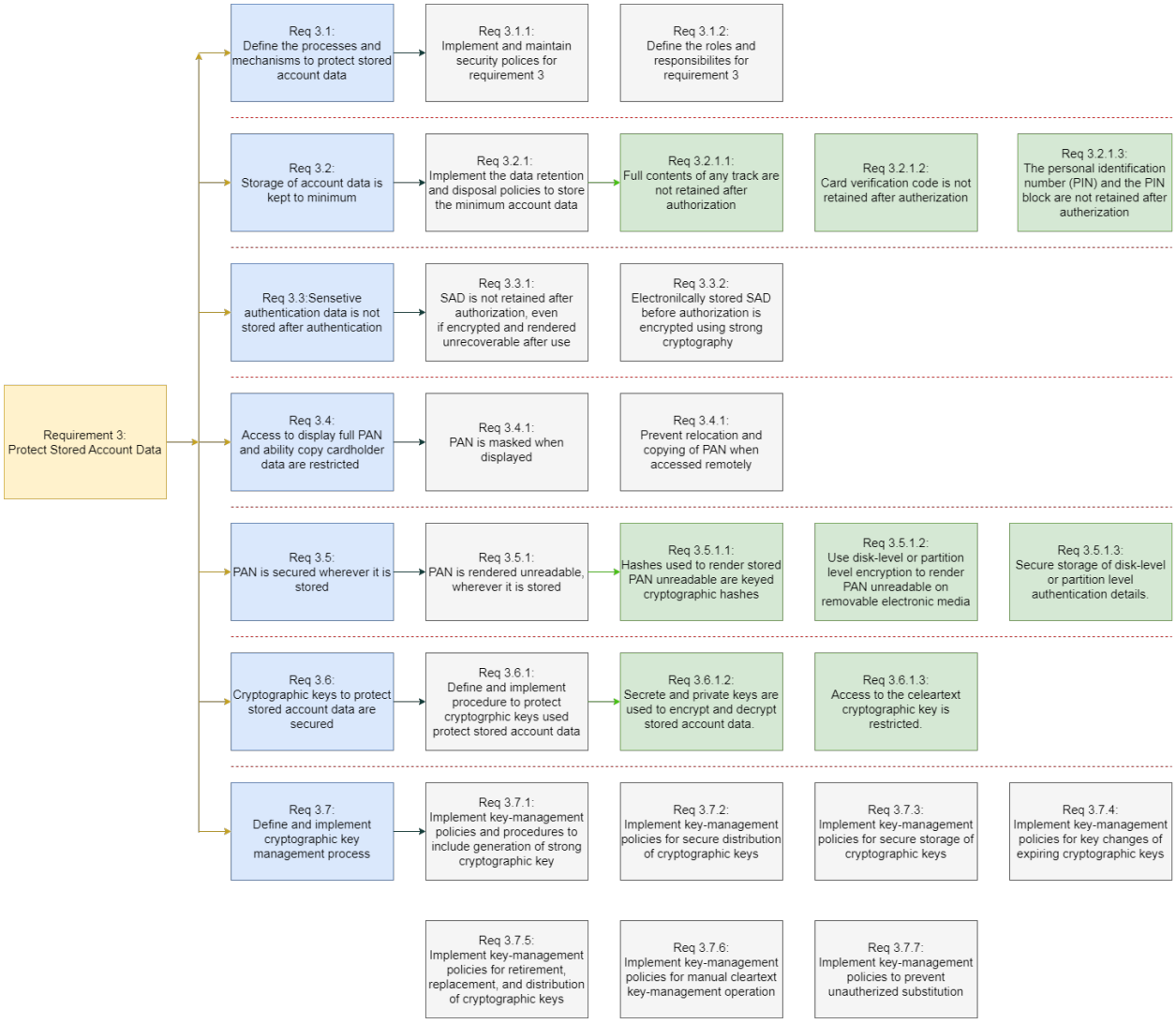
要件 2 のための Qualys ソリューション VMDR, CM, PC, FIM, WAS, EDR, SCA

要件 2 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
2.2.1	✓	✓							✓		✓	
2.2.2	✓	✓	✓								✓	
2.2.3		✓									✓	
2.2.4		✓									✓	
2.2.6		✓	✓						✓			
2.2.7			✓		✓						✓	
2.3.2		✓									✓	

PCI DSS 要件 3

保存されたアカウント データの保護: アカウント データの保存を最小限に抑え、機密認証データ (SAD) を削除し、カード所有者データへのアクセスを制限し、カード所有者データを暗号化、切り捨て、トークン化して、カード所有者データのセキュリティを確保する対策を実装します。



- Qualys は、保存されたデータを不正アクセス、セキュリティ侵害、その他のセキュリティ脅威から保護するために、強力なセキュリティ対策を採用しています。
- Qualys クラウドプラットフォームに保存されるデータは、256 ビットキーを使用した Advanced Encryption Standard（AES）を使用して暗号化されています。
- Qualys は、ハードウェアセキュリティモジュール（HSM）を使用した安全なキーストレージ、ロールベースのアクセス制御、多要素認証、データ環境の分離、ネットワークセグメンテーション、継続的な監視と監査などの手法も採用しています。

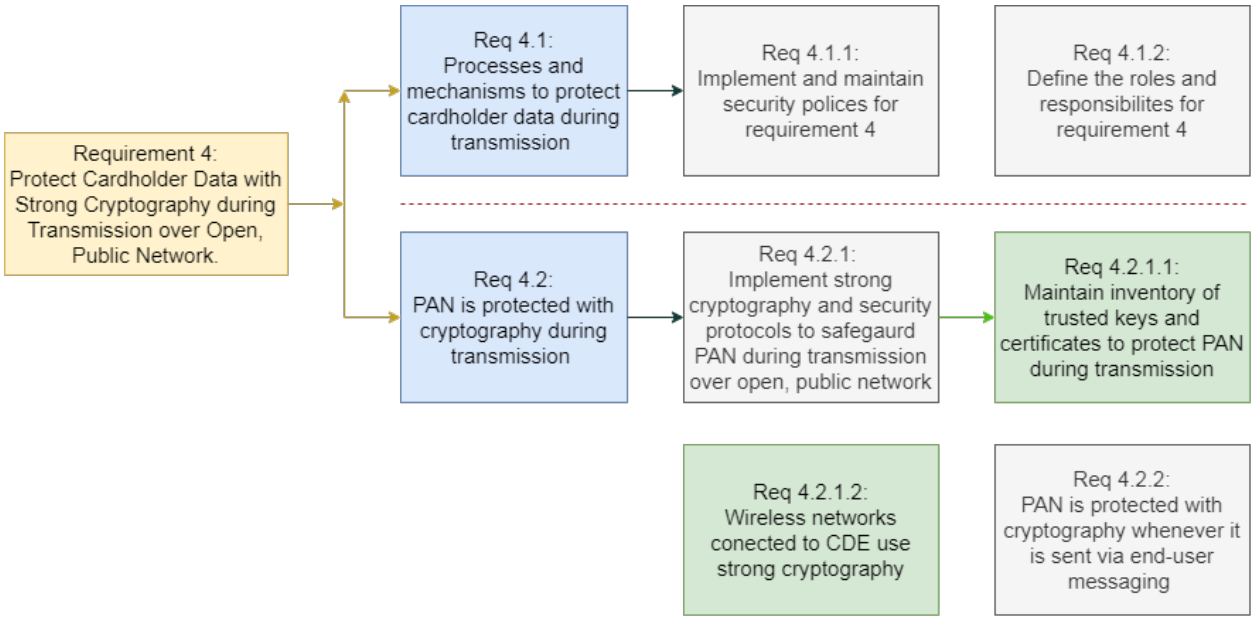
要件 3 のための Qualys ソリューション VMDR, CM, PC, FIM, GAV, CSAM

要件 3 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	CertView	WAS
3.2.1	✓								✓			
3.2.1.1		✓										
3.2.1.2		✓										
3.2.1.3			✓									
3.3.1		✓										
3.3.2		✓	✓									
3.4.2		✓	✓									
3.5.1		✓										
3.5.1.2		✓										
3.5.1.3			✓				✓	✓	✓			
3.6.1.2			✓									
3.7.1		✓										
3.7.2			✓									
3.7.3			✓									
3.7.4			✓									
3.7.5		✓										
3.7.7			✓									

PCI DSS 要件 4

オープンなパブリックネットワーク経由での送信中に、強力な暗号化を使用してカード所有者データを保護: オープンなパブリック ネットワーク経由での送信中に、カード所有者データが強力な暗号化を使用して保護されていることを確認します。



- Qualys は、転送中および保存中のデータのセキュリティを確保するために、包括的なデータ暗号化手法を採用しています。
- 転送中のデータについては、Qualys は TLS（Transport Layer Security）と HTTPS を使用して、お客様の資産およびアプリケーションから Qualys クラウドプラットフォームに転送されるデータを保護します。TLS は、256 ビット鍵の AES（Advanced Encryption Standard）などの強力な暗号化プロトコルとアルゴリズムを使用します。
- Qualys クラウドプラットフォーム内に保存されるデータは AES-256 で保護され、高度なセキュリティが確保されています。
- Qualys は、暗号化鍵の生成、保存、保護のために、堅牢な鍵管理手法も採用しています。
- これらの暗号化手法に加えて、Qualys はアクセス制御、データセグメンテーション、継続的な監視などの追加のセキュリティ対策も実装しています。

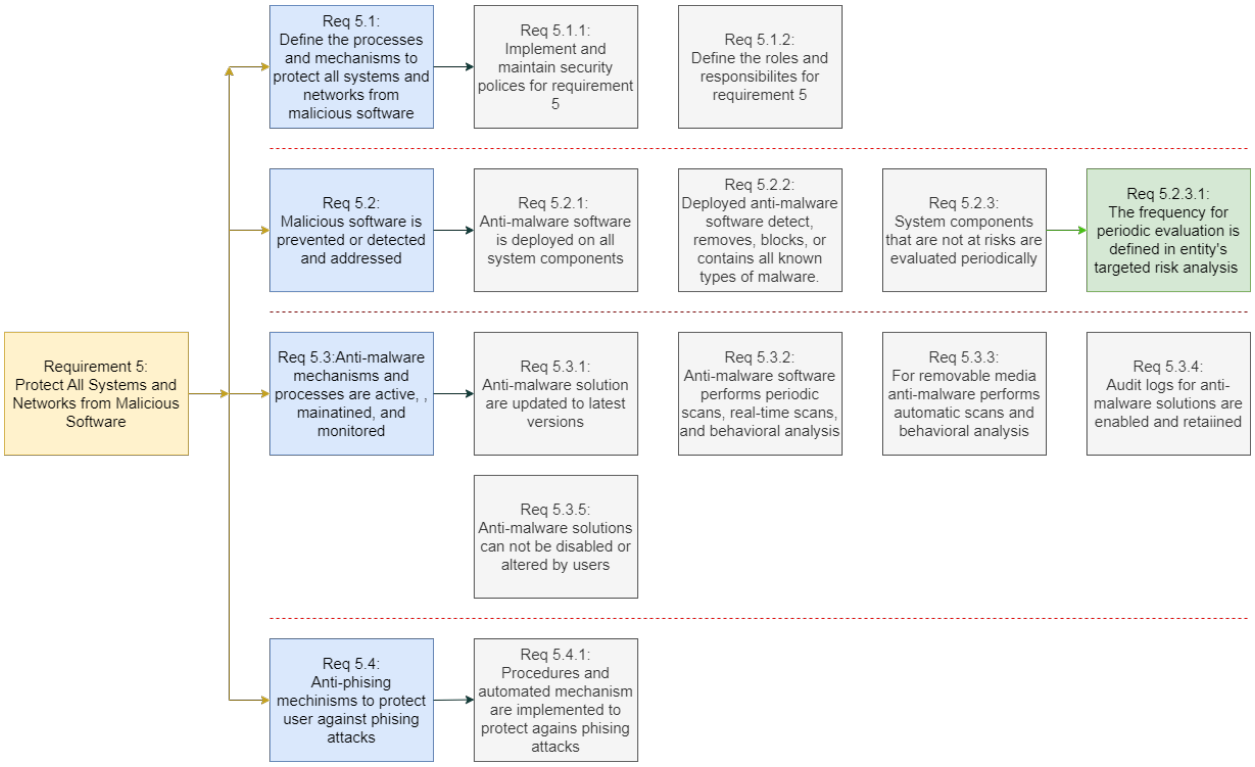
要件 4 のための Qualys ソリューション PC, EDR, CertView

要件 4 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	CertView	WAS
4.2.1		✓			✓						✓	
4.2.1.1											✓	
4.2.1.2		✓			✓							
4.2.2		✓			✓							

PCI DSS 要件 5

すべてのシステムとネットワークを悪意のあるソフトウェアから保護:マルウェア、フィッシング攻撃、その他のセキュリティ脅威からシステムとネットワークを保護するには、明確に定義されたプロセスとメカニズムが必要です。また、進化する脅威から保護するために、これらのプロセスを継続的に監視・維持することも重要です。



Qualysは、統合されたクラウドプラットフォームサービスを通じて、お客様のシステムとネットワークを悪意のあるソフトウェアから包括的に保護します。詳細については、以下の点をご確認ください。

- Qualys は**マルウェア検出**機能を搭載し、エンドポイントとサーバー上の既知の悪意のあるソフトウェアをスキャンします。
- **Qualys の脅威インテリジェンス**により、最新のマルウェアの傾向や脅威からシステムを保護します。

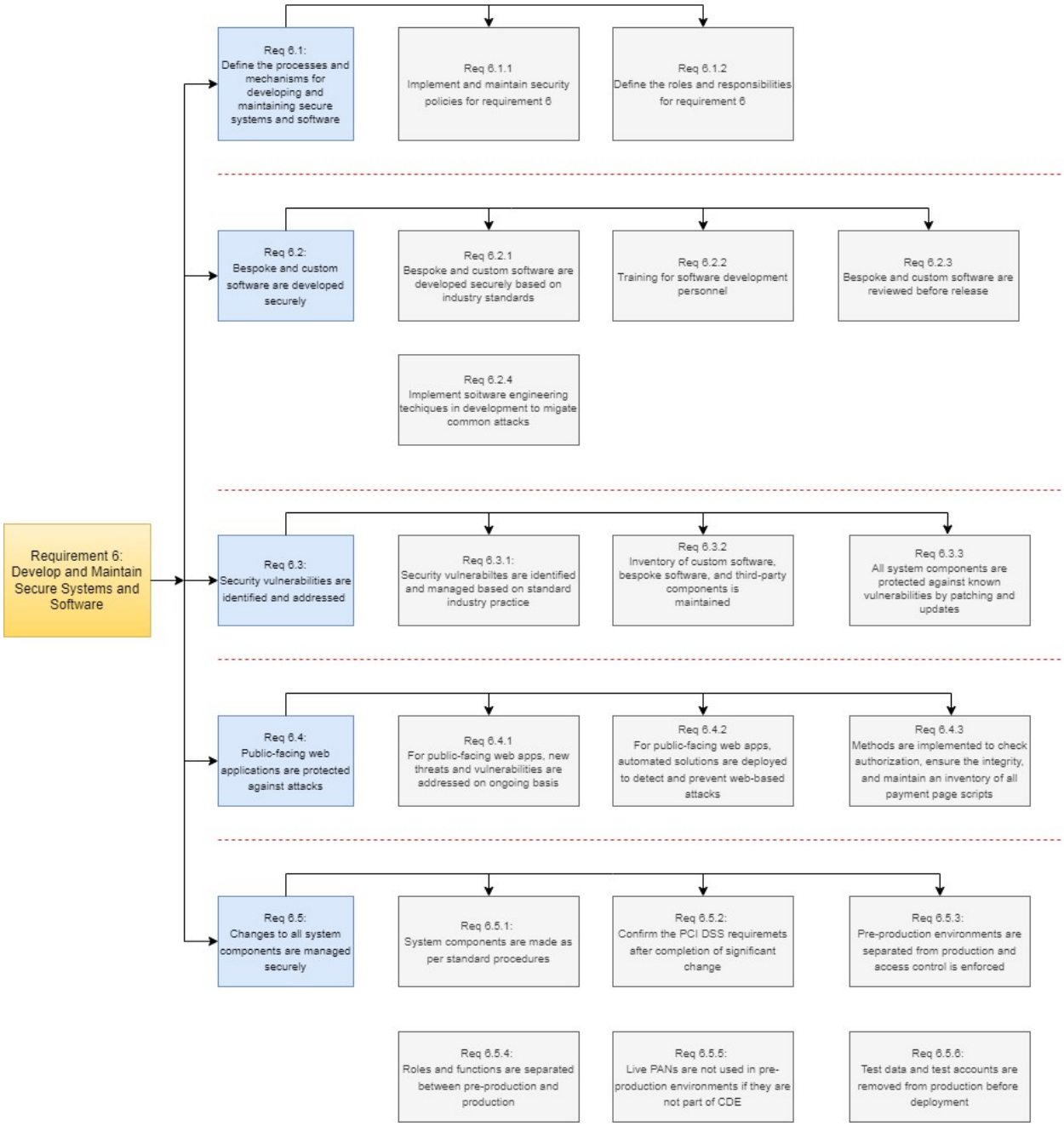
要件 5 のための Qualys ソリューション VMDR, CM, PC, FIM, EDR, SCA, PM, UD, CertView, GAV, CSAM

要件 5 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
5.2.1	✓				✓	✓			✓			
5.2.2	✓				✓							
5.2.3		✓							✓		✓	
5.2.3.1	✓											
5.3.1	✓	✓	✓		✓	✓			✓			
5.3.2	✓				✓				✓			
5.3.3	✓										✓	
5.3.4							✓	✓		✓		
5.4.1									✓			

PCI DSS 要件 6

安全なシステムとソフトウェアの開発と維持:セキュリティ上の脆弱性は決済データを危険にさらす可能性があります。ベンダー提供のパッチを定期的に適用し、安全なコーディングプラクティスを遵守してください。リスク分析に基づいてタイムリーなアップデートを実施し、システム変更を安全に管理してください。公開アプリケーションを攻撃から保護してください。



Qualys は、プロアクティブな監視、自動化ツール、コンプライアンスの実施、継続的な改善の実践を通じて、お客様のシステムとソフトウェアの安全な維持を保証します。

Qualys の以下のサービスを活用して、安全なシステムとソフトウェアを開発・維持できます。

Qualysは、お客様がセキュリティ体制を理解し、改善状況を追跡できるよう、以下の詳細なレポートと分析を提供します。：

- セキュリティの状況と傾向をリアルタイムで可視化します。
- さまざまな規制や基準への準拠を証明する詳細なレポートを提供します。

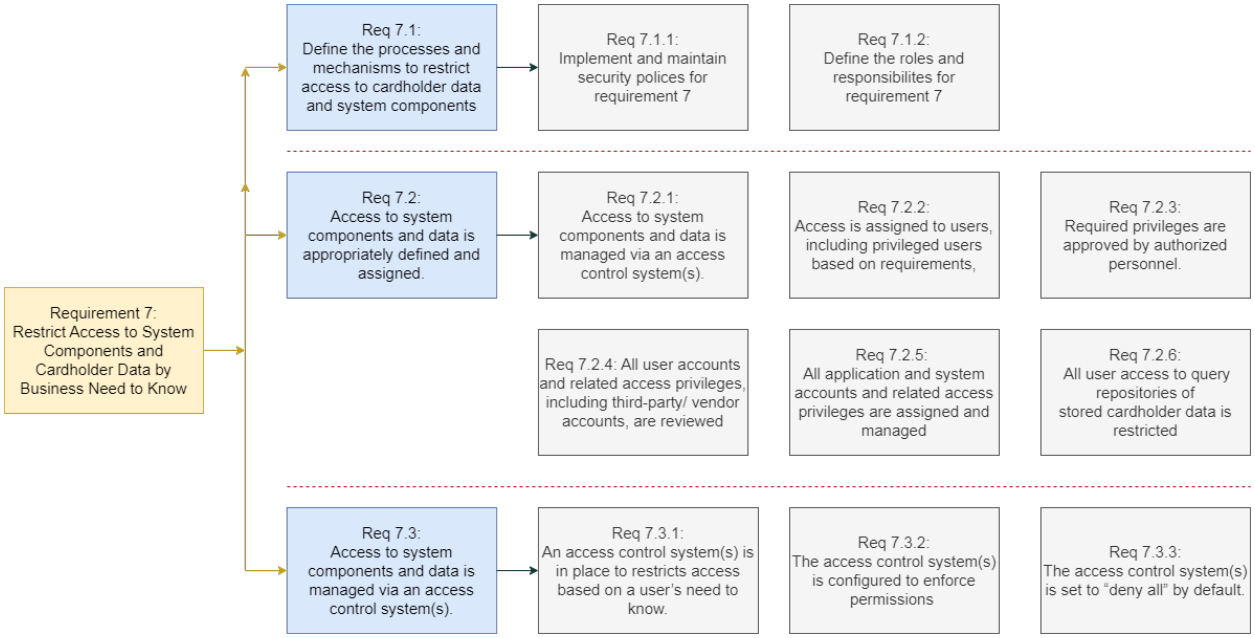
要件 6 のための Qualys ソリューション VMDR, CM, PC, FIM, WAS, SCA, PM, CAR, CertView, Admin, GAV, CSAM

要件 6 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	Admin	PM	GAV	SCA	CM	UD	WAS
6.2.1		✓									
6.3.1	✓										
6.3.2											✓
6.3.3	✓					✓			✓		
6.4.1									✓		✓
6.4.2		✓				✓		✓			
6.4.3											✓
6.5.2		✓									
6.5.3		✓			✓						
6.5.4					✓						

PCI DSS 要件 7

カード会員データへのアクセスを業務上の必要性に応じて制限:効果的なアクセス制御が不十分だと、重要なデータへの不正アクセスを許してしまう可能性があります。職務内容に則り、承認された担当者に必要最小限の権限を付与し、アクセスを制限するシステムを導入してください。アクセス制御プロセスは明確に定義・管理する必要があります。



- Qualys は、堅牢なアクセス制御メカニズムを組み合わせることで、ビジネスニーズに基づく情報提供の原則に基づいて、データアクセスの制限を保証します。
- Qualys は、詳細なロールベースのアクセスポリシー、きめ細かな権限設定、継続的な監視、詳細な監査ログの維持などの戦略を採用しています。

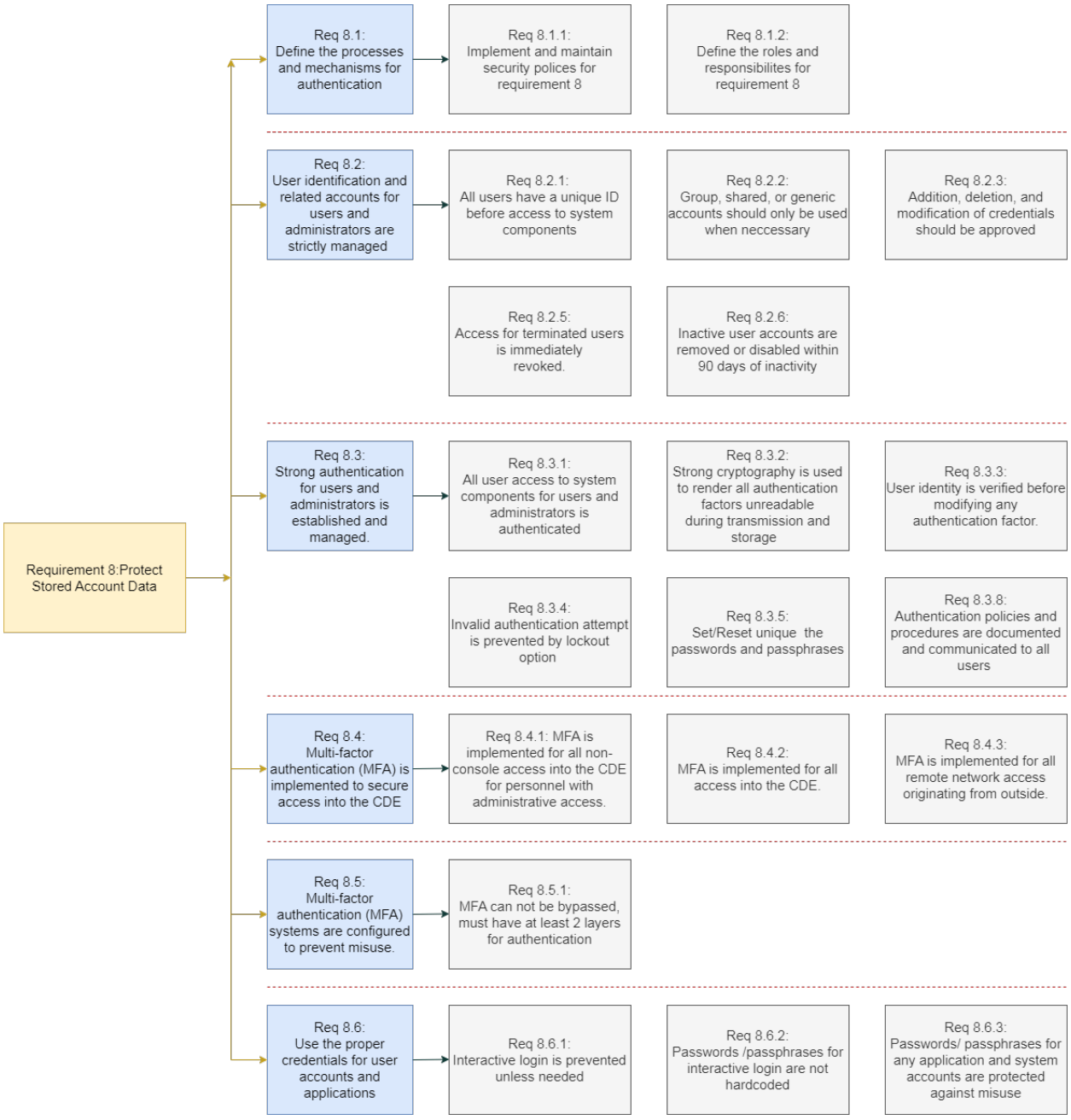
要件 7 のための Qualys ソリューション CM, PC, Admin

要件 7 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
7.2.1		✓										✓
7.2.2		✓										✓
7.2.3												✓
7.2.4												✓
7.2.5		✓										✓
7.2.6		✓										✓
7.3.1		✓							✓			
7.3.2		✓										✓

PCI DSS 要件 8

ユーザーを識別し、システムコンポーネントへのアクセスを認証:各アカウントに固有の ID を割り当てることで、重要なデータに対する操作が既知の承認済みユーザーによるものであることを確実にします。また、多要素認証などの強力な認証メカニズムとポリシーを実装し、維持することも重要です。



Qualysは、あらゆるセキュリティ状況において重要なデータを保護するための包括的なユーザー認証メカニズムの実装を支援します。以下の Qualys サービスは、このコンプライアンス要件の達成に役立ちます。

- Qualys 認証 API は、安全な API キー管理システムと OAuth2.0 などの業界標準の規制プロトコルを通じて、他のシステムとの統合のための安全な認証を提供します。
- Qualysは、セッション管理、アカウントロックアウトメカニズム、監査ログと監視、定期的なアクセスレビューなどのポリシーも採用しています。

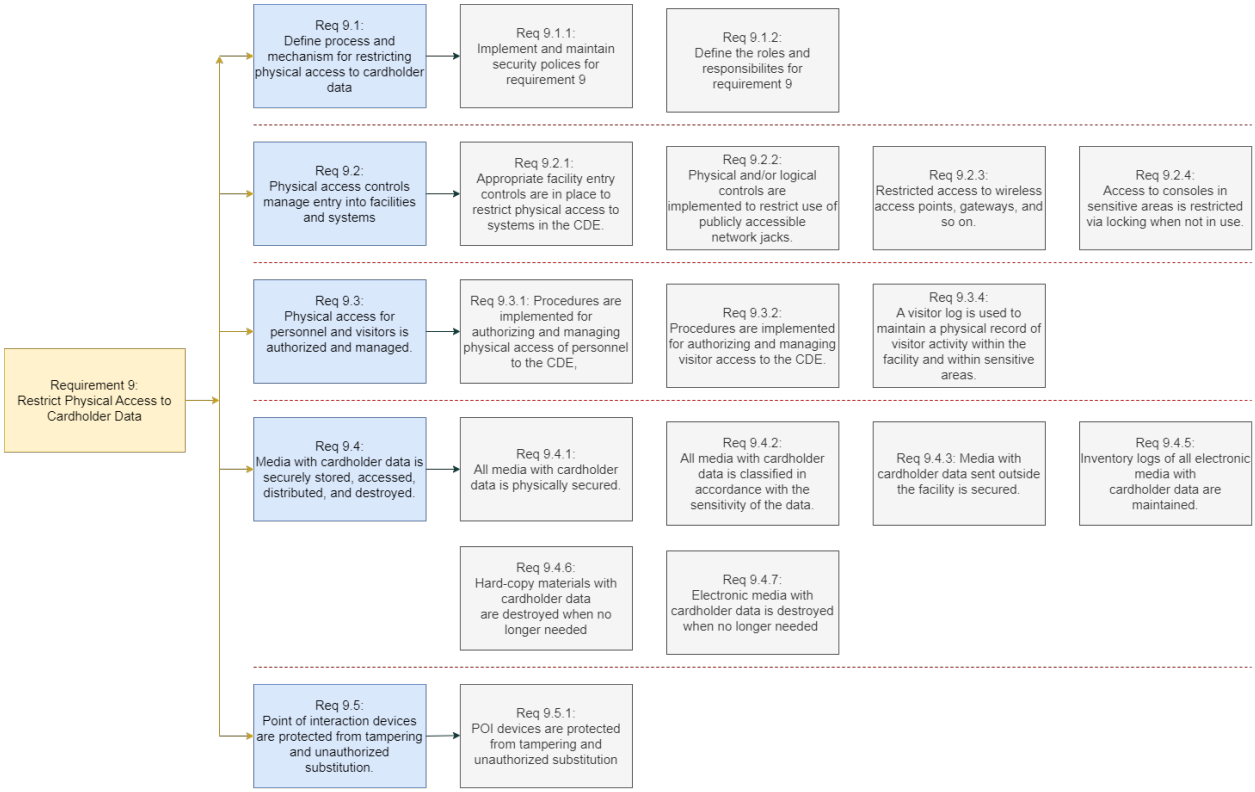
要件 8 のための Qualys ソリューション CM, PC, Admin

要件 8 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
8.2.1												✓
8.2.2		✓										
8.2.4												✓
8.2.5												✓
8.2.6		✓										
8.3.1		✓										
8.3.4		✓							✓			
8.4.1		✓										✓
8.4.2		✓										
8.4.3		✓										
8.6.1									✓			

PCI DSS 要件 9

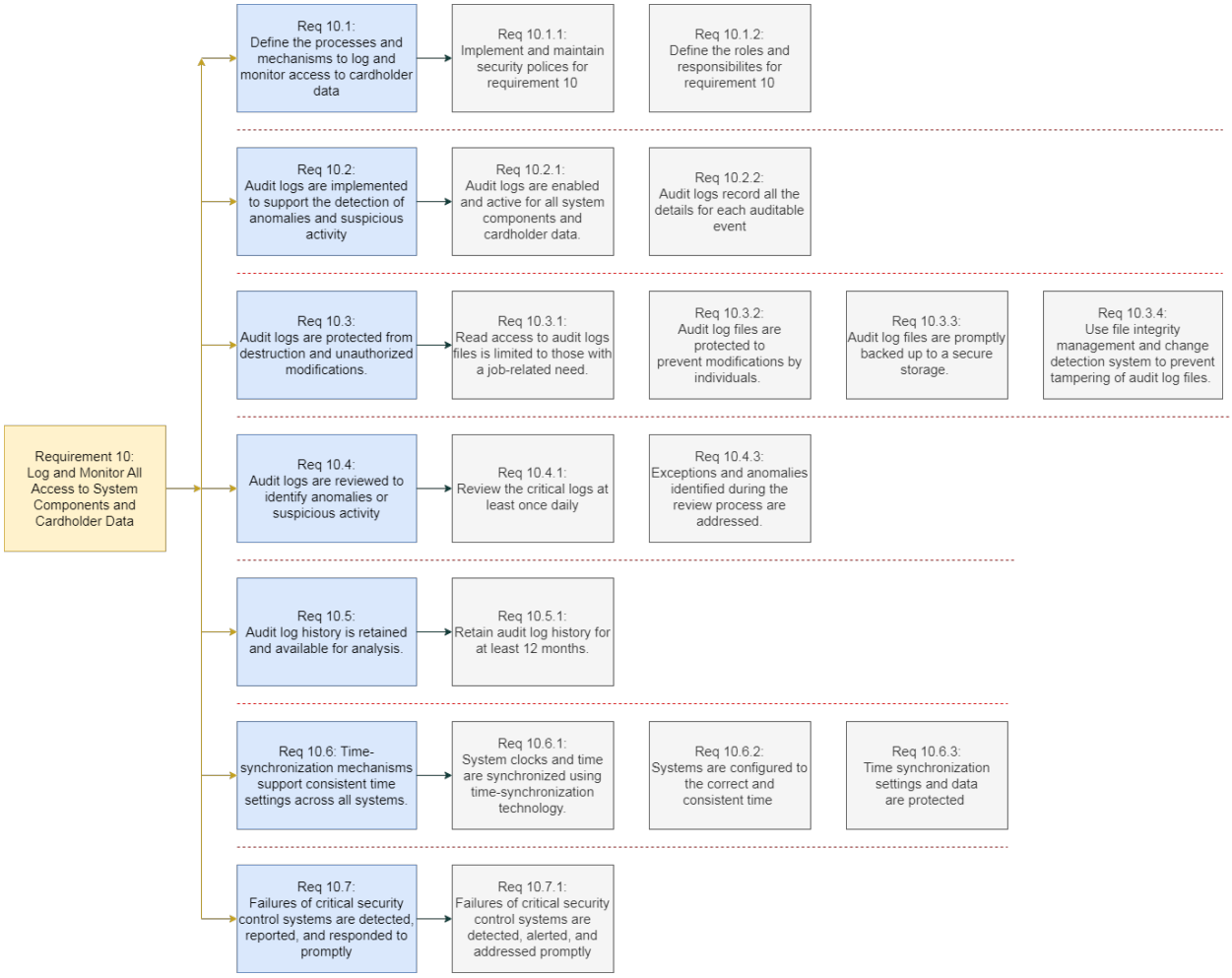
カード会員データへの物理的アクセスを制限:カード会員データ、またはこれらのデータを保存、処理、または送信するシステムへの物理的アクセスは、悪意のある行為者による認証されていない物理的な侵入から完全に保護する必要があります。カード会員に関連するメディアにアクセス、保存、および破棄するためのポリシーとメカニズムを導入し、インタラクションポイント（POI）デバイスの改ざんを防ぎます。



Qualys はデジタル セキュリティに重点を置いていますが、組織はカード所有者のデータが保存されている領域へのアクセスを制限するために物理的なセキュリティ制御を実装する必要があります。

PCI DSS 要件 10

システムコンポーネントおよびカード会員データへのすべてのアクセスを記録・監視する:すべてのアクセスを監視し、追跡および評価のためのログを維持する方針と仕組みを実施します。組織は、重要なセキュリティ制御の失敗を報告するアラート機構を設定しなければなりません。また、すべてのアクセスログが不正な破棄や改ざんから保護されていることを確保します。



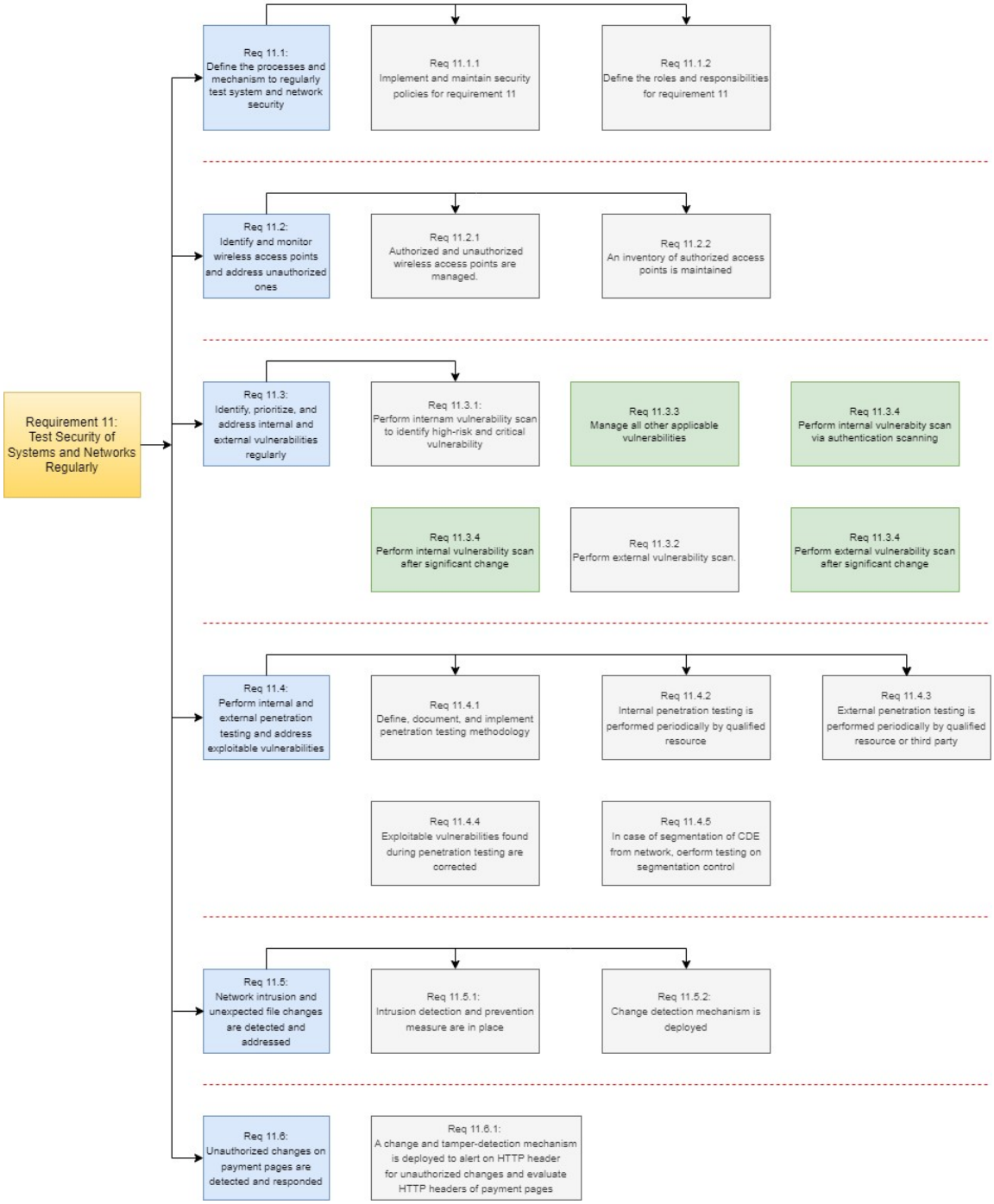
要件 10 のための Qualys ソリューション VMDR, CM, PC, FIM, SCA, PM, UD, GAV, Admin

要件 10 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	Admin
10.2.1		✓							✓			✓
10.2.2							✓			✓		
10.3.1												✓
10.3.3		✓										
10.3.4			✓									
10.4.1		✓									✓	
10.4.2	✓					✓						
10.6.3			✓									✓
10.7.1		✓	✓						✓			

PCI DSS 要件 11

システムとネットワークのセキュリティを定期的にテスト:すべてのセキュリティポリシーとメカニズムが効果的かつ最新であることを確認するためのテスト手順を整備します。これには、すべてのシステムとネットワークのテスト、内部および外部の脆弱性の特定、定期的な侵入テストの実施、重要なシステムファイルとソフトウェアへの不正な変更の検出と迅速な対応が含まれます。



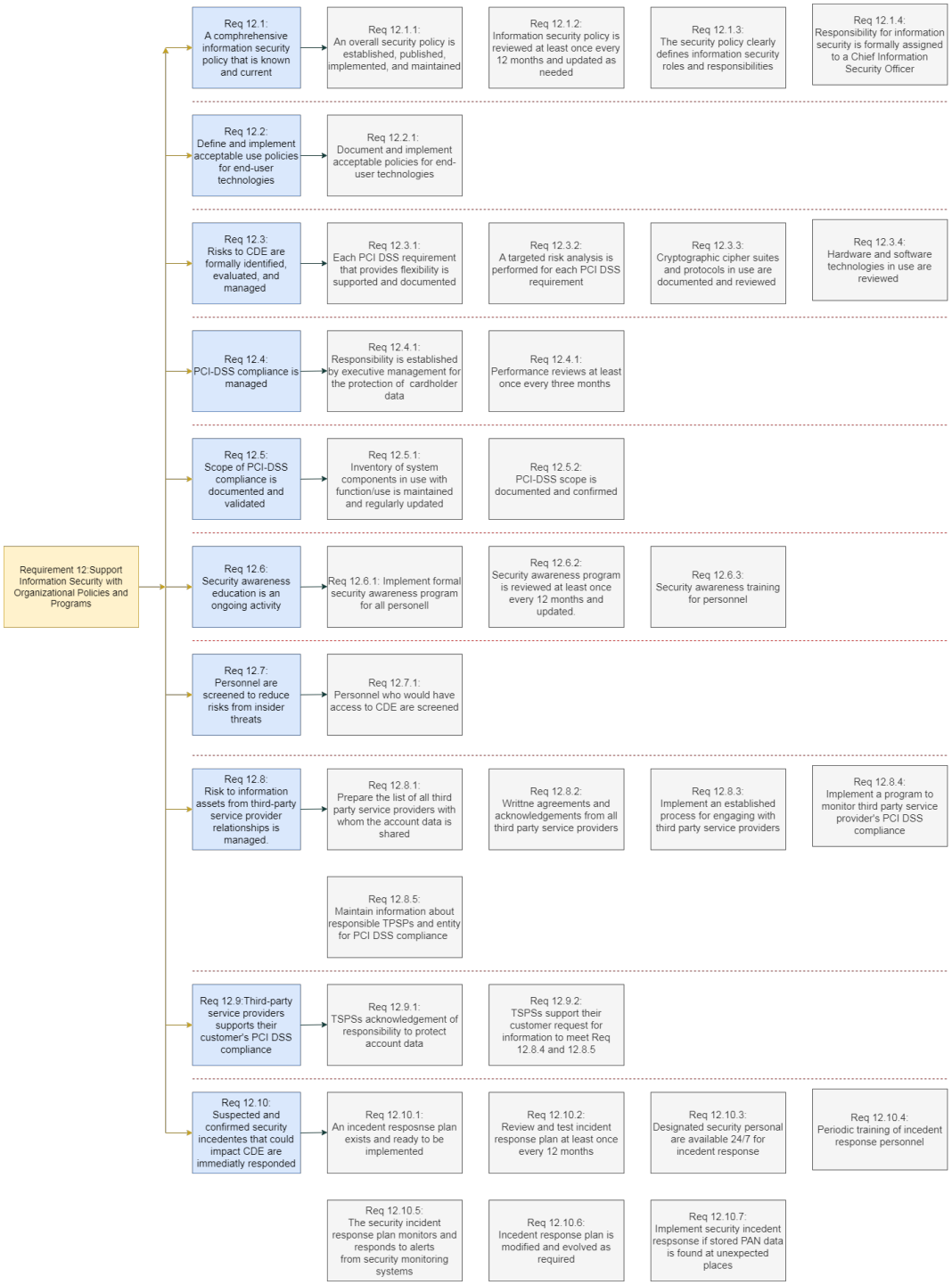
要件 11 のための Qualys ソリューション VMDR, CM, PC, WAS, EDR, PM, GAV, CSAM, WAS

要件 11 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	WAS	Admin
11.2.1					✓				✓			
11.2.2							✓	✓				
11.3.1	✓	✓										
11.3.1.1	✓	✓										
11.3.1.2		✓										
11.3.1.3		✓										
11.3.2	✓		✓		✓				✓			
11.3.2.1	✓				✓							
11.4.4						✓			✓			
11.5.1	✓		✓		✓	✓			✓			
11.5.2			✓									
11.6.1											✓	

PCI DSS 要件 12

組織のポリシーとプログラムによる情報セキュリティの強化：組織のセキュリティ維持に関わるすべての関係者がセキュリティリスクと PCI DSS コンプライアンスポリシーを認識できるよう、強力な情報セキュリティポリシーを実装します。ポリシーは徹底的なもので、あらゆるセキュリティインシデントを特定、報告、修復できるものでなければなりません。



要件 12 のための Qualys ソリューション CM, PC, FIM, EDR, SCA, PM, GAV, CSAM

要件 12 のための PCI コンプライアンスサポート

Req.	VMDR	PC	FIM	CAR	EDR	PM	GAV	CSAM	CM	UD	SCA	WAS
12.2.1		✓										
12.3.2		✓									✓	
12.3.3	✓	✓							✓			
12.3.4		✓										
12.5.1							✓	✓				
12.10.1		✓							✓			
12.10.5		✓	✓		✓	✓			✓		✓	
12.10.7		✓							✓			